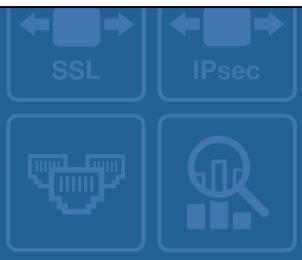
FORTINET

High Performance Network Security

FortiMail™ Release Notes

VERSION 5.4.3 GA



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

December 21, 2017

TABLE OF CONTENTS

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in this release.

Supported Platforms

- FortiMail 60D
- FortiMail 200D
- FortiMail 200E
- FortiMail 400C
- FortiMail 400E
- FortiMail 1000D
- FortiMail 2000E
- FortiMail 3000C
- FortiMail 3000D
- FortiMail 3000E
- FortiMail 3200E
- FortiMail VM (VMware vSphere Hypervisor ESX/ESXi 5.0 and higher)
- FortiMail VM (Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2)
- FortiMail VM (KVM qemu 0.12.1 and higher)
- FortiMail VM (Citrix XenServer v5.6sp2, 6.0 and higher)
- FortiMail VM [AWS(BYOL)]
- FortiMail VM [Azure(BYOL)]

What's New

The following table summarizes the new features and enhancements in this release.

Features	Descriptions
Content disarm and reconstruction (License required)	MS Office and PDF attachments may contain potentially hazardous macros, active scripts, and other active contents. Starting from 5.4.3, FortiMail provides the capability to remove or neutralize the potentially hazardous contents and reconstruct the email messages and attachment files.

Minimal DNS TTL	The following CLI command has been added to overwrite the TTL of cached DNS records in case the TTL of the records is very short:
	`config system dns`
	`set cache-min-ttl <time_in_seconds>`
	`end`
	For details, see the FortiMail CLI Reference.

Enhancement to system quarantine folder admin access	In the admin access profiles, different admin users can be assigned to access different system quarantine folders.
SMTP delivery preference for IPv4 or IPv6 addresses	When FortiMail delivers email to a host name, it does DNS AAAA and A record lookup. However, if the AAAA record does not exist, the extra AAAA DNS lookup for IPv6 addresses will potentially cause email delivery delay. New CLI commands are added to control whether the IPv4 or IPv6 addresses should be used first. For details, see the FortiMail CLI Reference.

Special Notices

TFTP firmware install

Using TFTP via the serial console to install firmware during system boot time will erase all current FortiMail configurations and replace them with factory default settings.

Monitor settings for web UI

To view all objects in the web UI properly, Fortinet recommends setting your monitor to a screen resolution of at least 1280x1024.

Recommended browsers on desktop computers for administration and Webmail

- Internet Explorer 11 (Windows 7) and Edge (Windows 10)
- Firefox 52 to 54
- Safari 9 to 10 (Mac OS X)
- Google Chrome 53 to 59

Recommended browsers on mobile devices for webmail access

- Official Safari browser for iOS 9 to10
- Official Google Chrome browser for Android 5 to 7

FortiSandbox support

The current FortiMail release requires FortiSandbox 2.1 or newer releases. FortiSandbox 2.3 or new releases are highly recommended.

Firmware Upgrade/Downgrade

Before and after any firmware upgrade/downgrade

- Before any firmware upgrade/downgrade, save a copy of your FortiMail configuration (including replacement messages) by going to *System* > *Maintenance* > *Configuration*.
- After any firmware upgrade/downgrade:
  - If you are using the web UI, clear the browser cache prior to login on the FortiMail unit to ensure proper display of the web UI screens.
  - The antivirus signatures included with an image upgrade may be older than those currently available from the Fortinet FortiGuard Distribution Network (FDN). Fortinet recommends performing an immediate AV signature update as soon as possible.

Upgrade path

For any 5.x release

Any 5.x release older than 5.2.3

↓

5.2.3 (Build 436)

↓

5.2.8 (Build 467)

↓

5.3.10 (Build 643)

↓

5.4.3 (Build 712)

For any 4.x release

Any 4.x release older than 4.3.6

↓

4.3.6 (Build 540)

↓

5.2.3 (Build 436)

↓

5.2.8 (Build 467)

↓

5.3.10 (Build 643)

↓

5.4.3 (Build 712)

After every upgrade, verify that the build number and branch point match the image that was loaded by going to *Dashboard* > *Status* on the Web UI.

Firmware downgrade

Downgrading from 5.4.3 to 5.x or 4.x releases

Downgrading from 5.4.3 release to any 5.x or 4.x release is not fully supported. If you have to downgrade, follow these steps:

1. Back up the 5.4.3 configuration.
2. Install the older image.
3. In the CLI, enter `execute factoryreset` to reset the FortiMail unit to factory defaults.
4. Configure the device IP address and other network settings.
5. Reload the backup configuration if needed.

Resolved Issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Antivirus/Antispam/Content

Bug ID	Description
460499	DKIM check causes mailfilterd crashes.
462226	When clicking to delete all spam email on a quarantine report, on the popup window, all the deleted email are displayed with the same subject name.
448879	Unable to release quarantined email using the search function.
461557	Quickly deleting a released email from multiple recipients may cause some recipients fail to received the released email.
461176	The block lists are checked first, instead of the safe lists.
461131	Domain part in <user>@<domain> in email body should not be included for URI scanning with "strict" settings (that is, to scan for absolute URIs only). Only the aggressive settings scan for both absolute and reference URIs.
457624	RCPT To checking in a recipient policy does not differentiate between main domains and associated domains.
455950	Wildcard in banned words does not work for Japanese words.
457291	Access control rules with reverse DNS lookup do not work for email with attachments.
465528	PDF content scan triggers PDF embedded file check.
461719	Non-final actions in the action profile for URI filters fall back to "personal quarantine".
457655	Some HTML contents fail to trigger dictionary profiles.

System

Bug ID	Description
461987	Webmail language cannot be customized.
460419	Port2 IP address is changed from 0.0.0.0/0 to 192.168.2.99/24 after upgrading from 5.3.11 to 5.4.2.
463208	Unable to import users in .csv files in server mode.
459590	Unable to back up configurations using SCP.
457236	Unable to create sender address rate control exempt list on the admin GUI.
457290	Generated local certificates miss some fields such as Country, City, and OU fields.
463568	FortiMail-3000E RAID beep alarm does not stop in some situations even though the rebuild has

Bug ID	Description
	completed. The following diagnose command has been added to temporarily silence the alarm. The alarm should clear once the failure event has be rectified. `diag system raid-silence-alarm`
461160	FortiMail needs to send protected domain names to FortiSandbox, which uses this information for submission limitation purpose.

Known Issues

The following table lists some minor known issues. .

Bug ID	Description
307919	Webmail GUI for IBE users displays a paper clip for all email although the email has no attachments.
381511	IBE messages are not signed with DKIM although DKIM signing is enabled.

Image Checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from Fortinet Customer Service & Support. After logging in to the web site, near the bottom of the page, select the *Firmware Image Checksums* button. (The button appears only if one or more of your devices have a current support contract.) In the File Name field, enter the firmware image file name including its extension, then select *Get Checksum Code*.

Figure 1: Customer Service & Support image checksum tool